E-Voting on the Blockchain

THE JBBA

ESSAY

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-1-2-(3)2018

E-Voting on the Blockchain

Kevin Curran[1] PhD
School of Computing, Engineering and Intelligent Systems, Ulster University, UK
Correspondence: kj.curran@ulster.ac.uk
Received: 3 September 2018 **Accepted**: 11 September 2018 **Published**: 14 September 2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
KC [1] prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract

Building a secure electronic voting system is a difficult task. The US Pentagon dropped their proposed online voting system which would have given overseas military personnel the opportunity to vote in the elections in 2005, citing the inability to ensure the legitimacy of votes as the reason. There is however a new cry in the wild to deploy a voting blockchain. The blockchain serves as a public ledger of transactions which cannot be reversed. The all-important consensus of transaction (i.e. legitimate votes) is achieved through 'miners' agreeing to validate new records being added. Whenever a new insertion is to be made e.g. votes, then a new transaction record is created by a voter adding details of their cast vote to the blockchain. Should it be deemed a valid transaction then the new vote is added to the end of the blockchain and remains there forever. What is neat about this solution is the fact that no centralized authority is needed to approve the votes but rather a majority consensus. Here everyone agrees on the final tally as they can count the votes themselves & because of the blockchain audit trail, anyone can verify that no votes were tampered with and no illegitimate votes were inserted. This paper discusses the application of blockchain to voting.

Keywords: *blockchain, e-voting, government, voting, electronic voting*

JEL Classifications: *D72, D02*

1. Introduction

Blockchains have become an important technology in a relatively short-time [1, 2, 3]. It does have major implications in future online systems ranging from finance to medicine to military. Very few domains will not have a blockchain deployed in the coming years. A blockchain is a distributed database that maintains an ever-growing list of data records secured from tampering or revision. It is de-centralised avoiding a single point of failure with the group working together to confirm legitimate new transactions [4]. It is composed of data structure blocks where each block holds batches of individual transactions and the results of any blockchain executables. These blocks contain a timestamp and a link to a previous block. The blockchain therefore serves as a public ledger of transactions which cannot be reversed (or without great difficulty). Blockchain technology can transform key aspects of society such as smart contracts to make micropayments for use more cost effective or in the music industry to enable data sharing among the value chain from artist to final consumer realizing and releasing more value [5]. What is neat about blockchain is the fact that no centralised authority is needed to approve the transaction but rather a majority consensus [6,7]. Now, for the first time we can have a system of barter - a system of storage - a lottery system etc - running globally with no central ownership, semi-anonymous - yet full of trustworthy transactions which cannot be cheated. That really does change things in many domains [8].

Adopting Distributed ledger technology (aka blockchain) is not simply a technological decision but also a business decision and therefore any real-world use case must also solve real problems for organizations which deploy one [9]. One of the most valid domains for a blockchain is for voting. Building a secure electronic voting system is a difficult task. Many governments have tried to roll out electronic systems but example after example shows that there were flaws. Governments are keen to see an IT solution as the costs of elections are non-trivial and in recent years voter apathy has been on the increase, especially among the younger computer savvy generation. The importance of voting deems it a crucial system that must execute without failure. There is however a new hope in the creation of a decentralised platform which can address many of the weaknesses which were inherent in traditional electronic voting systems.

Of course, at this time, there are many who believe a

blockchain can be applied in most domains when, a Blockchain only makes sense when multiple mutually mistrusting entities wish to interact & change the state of a system and are not able to agree on an online trusted third party [10, 11]. Some will claim that the only true legitimate use case for a blockchain is cryptocurrencies however others think that the ledger's decentralised, tamper-proof nature makes it safe enough to allow fraud-free online elections. An interesting side effect of a blockchain is that it could allow for continuous voting e.g. casting a vote every week or month. This paper explores the application of blockchain for electronic voting.

2. The case for a blockchain for voting

One of the most valid domains for a blockchain is for voting [12, 13, 14, 15]. Blockchain distributes individual voting information across thousands of computers globally making it impossible to alter or delete votes once they have been cast. This approach promotes greater trust between voters and governments by protecting their data and privacy. Trust is inherently created by having the user in control over their data. Platforms like this allow allows citizens to cast their votes on smartphone apps, rather than having to queue up at polling stations. Implementing a blockchain does not require governments to completely rebuild their systems but rather their existing platforms can be re-modelled to fit. All signs point towards a shift towards decentralised remote participation as opposed to traditional centralised gatherings at public polling stations.

A Blockchain architecture specifically addresses one of the most difficult factors challenging electoral integrity – trust. Blockchain ensures trust is distributed amongst a set of mutually distrustful parties, all of whom are potentially adversarial, that participate in jointly managing and maintaining the cryptographically secure digital trail of an election. By distributing trust in this way, blockchains create a trustless environment whereby the amount of trust required from those participating in an election is minimized. The major weakness of blockchain in providing a solution for most business domains is that storing data or large files on the blockchain a non-starter as it can barely sustain small strings of text that simply record a balance transfer between two parties. However, the Interplanetary File System (IPFS)[1] is an interesting project that could provide much of the infrastructure needed for blockchain content storage as it provides a permanent, decentralized Web where links do not die, and no single entity controls the data. Organisations can add any data to it and in return receives a unique identifying hash. IPFS is a content-addressed system, in contrast to the Web, which is an IP-addressed system. It provides a decentralized way of storing files on a blockchain but giving more control, securely identifying content & providing rich programmatic interactions. It has potential but still in preliminary stages.

Ultimately, any blockchain implementation for e-voting must satisfy as follows [16, 17, 18].

- **Public Verifiability** Everyone involved can see the voting process (recorded on blockchain) & verify the election's outcome.
- **Individual Verifiability** All voters can verify their ballot has been recorded in the final tally.
- **Dependability & Consistency** The blockchain should be non-attackable and accept the same outcome of the election.
- **Auditability** The voting process on the blockchain is auditable after the election by the public or third-parties
- **Anonymity** All ballots have no connection with their voters (but each voter can verify their cast vote)
- **Transparency** The blockchains transparency ensure the procedure is open to public scrutiny.

3. E-Voting Blockchain Projects

Some projects which are currently seeking or have implemented e-voting implementations on Blockchain include the following:

3.1 Luxoft

Luxoft Holding[2], a global IT service provider of technology solutions aims to deliver an e-voting platform that enables the first consultative vote based on blockchain in the city of Zug, Switzerland. As one of the founding members of The Crypto Valley Association, which aims to build the world's leading blockchain and cryptographic technology ecosystem, Luxoft partner with organizations working on government-based blockchain service solutions and invite them to jointly create Blockchain for Government Alliance. In the pursuit of driving the adoption of blockchain-based services in government, Luxoft is striving to establish a blockchain for government alliance and hence promote blockchain use-cases in public institutions. Zug already accepts cryptocurrency for services and has digitized the blockchain based solution e-Vote, including the platform itself, software and algorithms is built on Hyperledger Fabric. Integrated with Zug's Ethereum-based digital ID registration application, residents are hereby allowed to cast votes on the blockchain.

The solution claims to use an innovative encryption technology that anonymizes the votes and allows tamper-proof tally and secure audit. With the help from the Lucerne University of Applied Sciences and Arts, Amazon AWS and n'cloud.swiss, the platform is deployed on three different data centers in the cloud.

Two of these are in Switzerland and one in Ireland. By distributing the data into three different data centers, security and data loss risks are distributed geographically for robustness.

3.2 IIT Bandung

IIT Bandung researchers [19] outline a recording of voting result using blockchain algorithm from every place of election. Unlike Bitcoin with its Proof of Work, they proposed a method based on a predetermined turn on the system for each node in the built of blockchain. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once

validated, then the database is updated with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

The blockchain permission protocol used is a distributed record-keeping system operated by known entities, in other words having the means to identify nodes that can control and update data together in achieving the participants trust goals. The known entity in this system is any node that has been registered before the process runs, with the public key on each node owned by all the nodes in the system. Any data that is broadcast by the node that gets a turn is always verified and updated its data by the recipient. The verification system performed by all receiving nodes can identify if there are previous hashes and / or public keys that are not registered in the database. The counter-time system becomes a parameter when there are nodes that have interference functioning in accordance with the design. Nodes that experience interference can perform manual data or system broadcast can be repeated to update data when the process has reached the last turn node. Each previous hash that is used by the block in the system has proven the same as the hash value on the calculation results using the data in the previous block. Each hash value in the previous block has been included in the calculation of hash values by the block that gets a turn on the system, making anyone who wants to change the data in the database will have difficulty because if one data is changed it must make changes to data on other block.

3.3 Ethereum Blockchain Trustless Voting

Fernado Lobato open sourced a voting system[3] as a smart contract running on Ethereum that uses threshold keys and linkable ring signatures to provide a transparent and robust system that could be implemented for medium size elections. Each voter is in control and can monitor his vote while remain anonymous amongst a set of users. The protocol minimizes centralization using threshold cryptography which allows for the voting to be tallied by anybody and does not require every user to vote for tallying to be precise. The execution of the protocol via the Ethereum protocol. They deployed the contract to the Ethereum test network and provided some analysis on feasibility and costs in the supporting paper[4]. The voting scheme is divided into the following phases after being deployed on the blockchain.

- Setup - Election authority uploads all information about the election. Length of voting and registration periods, threshold key for voters to encrypt their votes and the voting options.
- Registration - At this phase any voter can go with the election authority and request his public key be included into the set of public keys eligible to vote.
- Voting - At this phase any previously registered voter and submit an encrypted vote with the threshold key published in the contract with a ring signature of all the public keys registered in the sub ring.
- Finished - Once the voting phase is over all the third parties holding secrets can submit them to the blockchain. When all the secrets are in the contract, anybody can download and reconstruct the private key.
- Ready to Tally - Anybody can tally the result of the election.

The online repo contains Solidity contracts to represent election, Python scripts to compile and deploy., Javascript files for testing, a small web application to run the election scheme, Python program for working with linkable ring signatures and a Python program for working with threshold encryption. Development was done in a private Ethereum network deployed in two computers. The code has a set of scripts and documentation on how to recreate an Ethereum private network. The final tests were done in Ethereum official test network (Ropsten). There are 3 Ethereum test networks. Two of them use an alternative to Proof-of-Work called Proof-of-Authority where only certain nodes can mine transaction in a semi trusted environment that is not as energy consuming. They used Ropsten which mimics Ethereum current live network.

3.4 Public Votes

PublicVotes[5] is a freely available simple voting application built with Meteor that utilizes the Ethereum Blockchain to create a provably fair and transparent voting system. All votes of participants are recorded (by proxy) into the Blockchain for the world to verify. The application is not fully decentralized, since the design goal was to create an application that is easy to use for people outside the Ethereum space. The entire platform is built on Meteor with one smart contract coded in Solidity that is used for placing a poll into the Blockchain and for casting the votes. Anyone with a small amount of Ether can create a poll. At PublicVotes, the creator of the poll pays for the creation of the poll and for all votes.

A poll consists of the following information:

- Title: Mostly a question that indicates what the users are voting about.
- Description: A more comprehensive description that explains to the users what the vote is exactly about.
- Options: The actual voting options for the poll.
- Public Poll: The user can choose if the poll should be public or not. If the poll is private, only people with the link can participate in the vote.
- Vote Limit: Limits the number of people that can participate in the poll.
- Time Limit: This is a requirement as the account will eventually run out of Ether.

Once the creator has entered this information, he/she is required to send a specified amount (0.2 Ether to be exact) of Ether to an address. All the accounts are generated on the client. This account is then stored in a local MongoDB collection and will be used for all future votes. Once the Ether have been received at the specified address, the poll is ready to go live and be deployed onto the Ethereum Blockchain. Once the contract has been mined, the poll will go live, and people can start voting. Once a vote has been received, the smart contract will record the vote into the Blockchain's event log. After voting, the user is redirected to /voted where there are statistics about the poll and the people who have voted.

3.5 Votem Proof of Vote

Votem Corp is a three-year-old blockchain-based mobile voting headquartered in Cleveland, Ohio. They have created a Proof of Vote protocol[6], an end-to-end voter verifiable (E2E) digital voting system that uses blockchain to ensure the verifiability, security, and transparency of an election. The protocol leverages an ElGamal re-encryption mix-net for anonymity, a multi-signature scheme for voter authentication and authorization, and verifiable distributed key generation and verifiable decryption for vote encryption and decryption. Their protocol is like other end-to-end voter verifiable (E2E) voting systems [18] in that:

- Voters encrypt their vote with an election-specific public key, post it to a public repository of votes, and achieve anonymity via a homomorphic cryptosystem.
- To achieve anonymity, the set of encrypted ballots is processed via a homomorphic cryptosystem and tallied with proofs of correct operations.

Proof of Vote differentiates itself from other voting and governance protocols by being designed from the ground up to explicitly optimize for the maximum level of verifiability, accessibility, security, and transparency of an election system deployed in the real world. It offers substantial advantages over more traditional E2E systems [20] via the use of blockchain and a multi-party signature scheme for voter authentication and authorization, aiming to be a mature and tried technological blueprint for how societies, governments, and organizations can build election systems and processes. Furthermore, Proof of Vote leverages blockchain to perform verifiable distributed key generation (for generating an election's public key), verifiable vote anonymization via mix-networks, and verifiable vote decryption. Every action that takes place as part of the Proof of Vote Protocol is realized as a transaction on the blockchain. This means that every action that takes places is verified in real-time by the entirety of the blockchain network and is inviolable once the transaction that represents that action is written to the blockchain. Furthermore, every action by a voter is fully visible to the voter and to every node at any time, maximizing visibility into an ongoing election without sacrificing the voter's anonymity.

4. Blockchain Types suitable for Voting

The major weakness of blockchain in providing a solution for most business domains is that storing data or large files on the blockchain a non-starter as it can barely sustain small strings of text that simply record a balance transfer between two parties [21, 22]. However, the Interplanetary File System (IPFS)[7] is an interesting project that could provide much of the infrastructure needed for storing data on the blockchain as it provides a permanent, decentralized Web where links do not die, and no single entity controls the data. Organisations can add any data to it and in return receives a unique identifying hash. IPFS is a content-addressed system, in contrast to the Web, which is an IP-addressed system. It provides a decentralized way of storing files on a blockchain but giving more control, securely identifying content & providing rich programmatic interactions. It has potential but still in initial stages.

A permissioned public shared blockchain would allow for the casting of votes quickly with prominent levels of trust and ultimately provide real-time publicly verifiable casting of votes by all engaged parties. It is therefore envisaged that a public permissioned ledger could be most applicable for e-voting. What makes the deployment of a permissioned public blockchain most applicable here is that we have a finite number of trusted parties who must be included in the blockchain for it to work e.g. voters, neutral observers & political organisations. A blockchain is suitable for several reasons which are not always the case when it comes to blockchain proposals. Here a blockchain would allow the casting of votes, the tallying and the verification of votes from the point of creation through the system of release and distribution. The assets are created from the beginning in a digital format and relate to the casting of votes. There is no requirement for millisecond transaction speeds for managing the assets. The solution is about allowing trusted third parties to cast votes and is, therefore, a good match for blockchain. Shared write access is required so that all parties can have a transparent record of what has occurred and when. This provides irrefutable proof that a cast vote is associated with an individual [23, 24].

Blockchain therefore looks like a viable solution to ease the strictures of existing traditional centralised solutions, however in practice what would be needed is the bringing together of representatives of all the activities in the voting value chain, from individual voters to the government agencies.

5. Conclusion

A valid route for an e-voting blockchain is through a permissioned public shared ledger. A permissioned, public, shared blockchain is a form of hybrid system that provide for situations where whitelisted access is required but all the transactions are viewable by the public. It applies here where only eligible voters can write to the network, but all transactions (i.e. votes) can be verified. A viable blockchain is Hyperledger Fabric which also have LevelDB which is a key value database allowing storage of data in the blockchain [25].

The Blockchains most compelling use cases are in areas such as cryptocurrencies, harvesting unused computer processors or e-voting where in each case, all parties involved are untrusted and transactions must be immutable. A permissioned, public, shared blockchain is a form of hybrid system that provide for situations where whitelisted access is required but all the transactions are viewable by the public. This provides the transparency needed in democracies. It applies here where only key players within the voting ecosystem can write to the network, but all transactions can be verified. A viable blockchain is Hyperledger Fabric which also have LevelDB which is a key value database allowing storage of data in the blockchain. The Interplanetary File System (IPFS) could be also be a feasible route as you can address substantial amounts of data with IPFS which is not the case with all blockchains which are concerned with transaction validation as opposed to storage of data [26].

E-voting however does bring some new problems such as ensuring privacy especially in the case of public permission less blockchains but there are solutions for that [27, 28, 29, 30]. Other problems include the speed by which transactions can be verified. For

instance, at this time Bitcoin and Ethereum can only process < 25 transactions per second compared, for instance, to Visa or Mastercard's thousands per second. This is not to say some countries have not experimented with blockchain for voting. In March, Sierra Leone recorded votes at 70% of the polling to the blockchain using a technology from Agora which anonymously stored votes in an immutable ledger. It provided instant access to the election results. Others such as Voatz, a startup out of Boston are building a platform for blockchain voting and are starting to experiment with New England open town meetings. The Nasdaq also recently ruled the Estonia experiment safe enough to allow firms to start using blockchain for proxy voting. So blockchain may be championed as the solution to many problems in vain, but one domain where it might make sense in the end - is electronic voting.

1. https://ipfs.io
2. https://www.luxoft.com/
3. https://github.com/fernandolobato/decentralized-blockchain-voting
4. http://aleph.com.mx/docs/blockchain_voting.pdf
5. https://github.com/domschiener/publicvotes/blob/master/contracts/contract.sol
6. https://github.com/votem/proof-of-vote
7. https://ipfs.io

References

[1] Amir, Y., Coan, B, Kirsch, J. and Lane, J. (2011) Prime: Byzantine replication under attack. IEEE Transactions on Dependable and Secure Computing, 8(4):564–577, 2011.

[2] Anane, R., Freeland, R. and Theodoropoulos, G. (2007) E-voting requirements and implementation, in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.

[3] Ayed, A. (2017) A conceptual secure blockchain-based electronic voting system, International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[4] Babaioff, M., Dobzinski, S., Oren, S. and Zohar, A. (2012) On Bitcoin and Red Balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce, pages 56-73. ACM, 2012.

[5] Barber, S., Boyen, X., Shi, E. and Uzun, E. (2013) Bitter to Better|How to Make Bitcoin a Better Currency. In Proceedings of Financial Cryptography, 2013

[6] Benet, J. (2014) IPFS - Content Addressed Versioned P2P File System, arXiv:1407.3561, 2014.

[7] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., and Felten, E. (2016) SoK: Bitcoin and second-generation cryptocurrencies, 36th IEEE Symposium on Security and Privacy, San Jose, CA, May 18-20 https://www.jkroll.com/papers/oakland15_bitcoin-sok.pdf

[8] Cachin, C., Guerraoui, R., and Rodrigues, L. (2011) Introduction to Reliable and Secure Distributed Programming (Second Edition). Springer, 2011.

[9] Christidis, K., Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. IEEE Access, Vol. 4, pp: 2292-2303, DOI: 10.1109/ACCESS.2016.2566339 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408

[10] Croman, K., Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M., Rohloff, K. (2016) On Scaling Decentralized Blockchains. Financial Cryptography and Data Security. FC, Berlin, Heidelberg:Springer, Vol. 9604, 2016.

[11] Gritzalis, D. (2002) Principles and requirements for a secure e-voting system, Computers & Security, vol. 21, no. 6, pp. 539–556, 2002.

[12] Harrison, T., Pardo, T. and Cook, M. (2012) Creating open government ecosystems: A research and development agenda, Future Internet, vol. 4, no. 4, pp. 900–928, 2012.

[13] Kroll, J., Davey, I., and Felten, E. (2013) The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, The 12th Workshop on the Economics of Information Security (WEIS 2013), Washington, US, June 10-11 2013 http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf

[14] Li, J., Liang, G., Liu, T. (2017) A Novel Multi-link Integrated Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication, KSII Transactions on Internet and Information Systems, 2017.

[15] Li, N., Li, T. and Venkatasubramanian, S. (2007) t-closeness: Privacy beyond k-anonymity and l-diversity. In ICDE, volume 7, pages 106–115, 2007.

[16] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007) l-diversity: Privacy beyond kanonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.

[17] Matthew, B. (2017) Public Evidence from Secret Ballots. International Joint Conference on Electronic Voting. Springer, Cham, 2017

[18] Maymounkov, P. and Mazieres, D. (2002) Kademlia: A peer-to-peer information system based on the xor metric. In Peer-to-Peer Systems, pages 53–65. Springer, 2002.

[19] Maull, R., Godsiff, P., Mulligan, C., Brown, A., Kewell, B. (2017) Distributed ledger technology: Applications and implications, Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

[20] McCorry, P., Shahandashti, S. and Hao, F. (2017) A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[21] Moura, T. and Gomes, A. (2017) Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263

[22] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008. http://bitcoin.org/bitcoin.pdf

[23] Quinn, A. (2018) Are online music platforms undermining the principles of copyright law? Journal of Intellectual Property Law & Practice, Volume 13, Issue 1, 1 January 2018, Pages 49-60 https://doi.org/10.1093/jiplp/jpx148

[24] Raskin, M. (2017) The Law and Legality of Smart Contracts (September 22, 2016). 1 Georgetown Law Technology Review 304 (2017). Available at SSRN: http://dx.doi.org/10.2139/ssrn.2842258

[25] Hanifatunnisa,R., Rahardjo, B. (2017) Blockchain based e-voting recording system design. The 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 26-27 Oct. 2017, DOI: 10.1109/TSSA.2017.8272896

[26] Sharma, P., Singh, S., Jeong, Y., Park, J.H. (2017) DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks, Communications Magazine IEEE, vol. 55, pp. 78-85, 2017.

[27] Swanson, T. (2015) Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. Report, available online, Apr. 2015. URL: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[28] Vukolic, M. (2016) The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In ´ Open Problems in Network Security, Proc. IFIP WG 11.4 Workshop (iNetSec 2015), volume 9591 of Lecture Notes in Computer Science, pages 112–125. Springer, 2016.

[29] Wang, K., Mondal, S., Chan, K. and Xie, X. (2017) A review of contemporary e-voting: Requirements, technology, systems and usability, Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017.

[30] Wüst, K., and Gervais, A. (2017) Do you need a Blockchain? IACR Cryptology ePrint Archive 2017 (2017): 375. https://eprint.iacr.org/2017/375.pdf

